United States Government Accountability Office

Report to Congressional Committees

July 2016

JOINT INFORMATION ENVIRONMENT

DOD Needs to Strengthen Governance and Management

On October 25, 2016, this report was revised on p. 25 to include the views of the Department of Defense Director, Operational Test and Evaluation, on responsibilities for JIE testing and assessments.

GAO-16-593

July 2016

JOINT INFORMATION ENVIRONMENT

DOD Needs to Strengthen Governance and Management

GAO Highlights

Highlights of GAO-16-593, a report to congressional committees

Why GAO Did This Study

For fiscal year 2017, DOD plans to spend more than $38 billion on information technology to support thousands of networks and millions of computers and other electronic devices connected to its networks. In August 2010, the Secretary of Defense announced an initiative, the JIE, to consolidate infrastructure in order to improve mission effectiveness, achieve savings, and improve network security.

A Senate Armed Services committee report included a provision for GAO to evaluate JIE. GAO's objectives were to (1) determine the extent to which DOD has effectively established scope, cost, and implementation plans for the initiative and (2) determine the extent to which DOD is executing effective oversight and governance of JIE. GAO compared JIE scope, cost, schedule, workforce planning, and security planning with leading program management practices, DOD guidance, and statutes. In addition, it compared JIE governance with leading practices.

What GAO Recommends

To help achieve JIE benefits and to enable effective oversight and governance, GAO recommends that DOD, among other things, fully define JIE's scope and expected cost, and take steps to improve workforce and security planning. DOD described steps it is taking or plans to take to address all of GAO's recommendations.

View GAO-16-593. For more information, contact Carol C. Harris at (202) 512-4456 or chac@gao.gov.

What GAO Found

The Department of Defense (DOD) plans to spend almost $1 billion by the end of this fiscal year to implement one element of the Joint Information Environment (JIE); however, the department has not fully defined JIE's scope or expected cost. Officials reported that assessing the cost of JIE is complex because of the size and the complexity of the department's infrastructure and JIE's implementation approach. However, without information about expected JIE costs, the ability of officials to oversee and make effective resource decisions is limited.

In addition, DOD has begun to assess the workforce needed to operate JIE, but has not determined the number of staff and the specific skills and abilities needed. DOD also lacks a strategy to ensure required JIE security assessments are conducted. Officials stated that the department has taken steps to address JIE personnel and security needs, but it does not have plans in place to address these existing gaps. As a result, DOD risks having a deficient security posture and not being able to ensure that it will have the appropriate workforce knowledge and skills needed to support JIE.

Table: JIE Elements

Element	Description
Single security architecture	Department-wide network security architecture
Optimized networks	Reduced number of networks
Identity and access management	Capability to create and administer identities across the department
Data centers and nodes	Core data centers and nodes to provide fast and secure connections to any application or service from any authorized network at any time
Software application rationalization and server virtualization	An effort intended to enable efficiencies and enhance information sharing
Desktop virtualization	A standardized virtual desktop environment
Mobility services	Integration of secure and non-secure communications and portable, cloud-enabled command and control capability
Enterprise services	Services, such as e-mail, provided in a common way across the department
Mission partner environment	A common set of standards, protocols, and interfaces to enhance data sharing with other agencies; allies; coalition partners; and private sector organizations

Source: GAO analysis of agency data. I GAO-16-593.

DOD has recently begun efforts to update the JIE governance structure and processes, including identifying the decisions and processes that it needs to document to support the effort. For example, it identified the need to document the process for planning and approving deployment of new JIE capabilities. However, the department has not established associated time frames. Until DOD establishes processes for helping to ensure that JIE decisions are based on reliable scope, cost, and schedule information, the department will face continued challenges in its ability to effectively oversee the initiative.

Contents

Abbreviations

CIO	Chief Information Officer
DISA	Defense Information Systems Agency
DOD	Department of Defense
IMS	integrated master schedule
IT	information technology
JIE	Joint Information Environment
JRSS	Joint Regional Security Stacks
NDAA	National Defense Authorization Act

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

July 14, 2016

Congressional Committees

The Department of Defense (DOD), one of the largest and most complex organizations in the world, spends billions of dollars each year to support its information environment. In fiscal year 2017, the department plans to spend more than $38 billion on its information technology (IT) environment, which includes thousands of networks and millions of computers and other electronic devices.

In August 2010, the Secretary of Defense announced an initiative—the Joint Information Environment (JIE)—to consolidate IT infrastructure in order to achieve savings and improve network security. As part of the JIE effort, DOD is currently implementing the Joint Regional Security Stacks (JRSS) project to replace about 1,000 legacy network security stacks with 48 standardized stacks at 25 locations around the world.[1] The goals of JRSS are to enable a DOD enterprise security architecture, enhance network command and control, and reduce the number of avenues (networks) vulnerable to a cyber attack.

Senate Armed Services Committee Report No. 113-176 included a provision for GAO to evaluate the JIE initiative.[2] Our objectives were to (1) determine the extent to which DOD has effectively established scope, cost, and implementation plans for JIE and (2) determine the extent to which DOD is executing effective executive oversight and governance of JIE.

To accomplish the first objective, we reviewed DOD's efforts to establish scope, estimate and baseline costs, and plan for implementing JIE. To evaluate planning, we examined DOD's efforts to estimate and baseline schedule and develop workforce and security assessment plans

[1]"Security stacks" comprise network security devices that perform routing and security functions. DOD is installing 23 JRSS stacks for its Non-secure Internet Protocol Router network and 25 for its Secret Internet Protocol Router network at the 25 locations.

[2]S. Rpt. 113-176 accompanied S. 2410, *Carl Levin National Defense Authorization Act for Fiscal Year 2015.*

consistent with leading program management practices, DOD policy and guidance, and legislative requirements. We also reviewed the department's efforts to establish cost and schedule estimates and baselines and develop security plans for JRSS.

To accomplish our second objective, we reviewed DOD documentation describing how the department is to manage and oversee JIE and interviewed relevant DOD officials, including those from DOD's Office of the Chief Information Officer, the Joint Staff, and United States Cyber Command to discuss JIE governance and oversight. We then compared management and oversight activities with leading practices for effective governance and oversight and summarized the extent to which DOD had executed key governance and oversight practices. More details about the objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from June 2015 to July 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DOD's mission is to protect the security of the United States and its interests around the world. The complexity of this mission is reflected in its information environment, which includes, according to DOD, about 15,000 networks, 10,000 operational systems, 65,000 servers, and 7 million computers and other electronic devices that are connected to its networks. Collectively, this environment supports DOD's 1.3 million military active duty and 742,000 civilian personnel, who are spread across the globe at more than 555,000 facilities.

Joint Information Environment

In August 2010, the Secretary of Defense announced an initiative to consolidate IT infrastructure to achieve savings in acquisition, sustainment, and manpower costs and improve the department's ability to defend its networks against growing cyber threats. This initiative became the DOD's Joint Information Environment.

In August 2012, the Joint Chiefs of Staff defined JIE's characteristics and goals. According to the Joint Chiefs, JIE is to be comprised of shared IT infrastructure, enterprise services, and a single security architecture to

improve mission effectiveness, increase security, and realize IT efficiencies.

In September 2013, DOD issued its strategy for implementing JIE,[3] which listed, in addition to the goals defined by the Joint Chiefs, the following goals:

- enhanced data access and information sharing within the department and with appropriate federal, state, international, and other partners;
- faster development and deployment of new warfighting support capabilities, including software applications; and
- more effective training.

JIE is to be comprised of several elements, including a single security architecture, and is to provide a new approach to operating and defending DOD's networks. For example, JIE is to enable network and system operators and defenders at every level to have visibility into the status of the networks and provide a common approach to how cyber threats are countered.[4] DOD components (e.g., military departments and defense agencies) that operate and maintain portions of the shared IT infrastructure will do so in accordance with enterprise technical and operational standards. Table 1 describes elements that are to comprise JIE.

Table 1: JIE Elements

Element	Description
Single security architecture	A common department-wide network security architecture to reduce the complexity and cost of network defense. Intended to improve interoperability across the network and increase network security by creating manageable network zones with consistent policies.

[3]*The Department of Defense Strategy for Implementing the Joint Information Environment* (Sept.18, 2013).

[4]According to *The DOD Cyber Strategy* (April 2015), providing the JIE single security architecture is a key objective to address the department's goal of defending the DOD Information network.

Element	Description
Optimized networks	A reduced number of networks to allow resources to be shared among multiple independent networks. Intended to improve the quality of network-based services and reduce costs.
Identity and access management	The capability to create and administer identities that uniquely and unambiguously distinguish people and machines on all networks, end-to-end across the enterprise. Intended to allow more effective monitoring of who is on the networks.
Data centers and nodes	As part of the federal data center consolidation initiative, DOD plans to designate each of the data centers that remain as one of several data center node types, including core data centers, installation processing nodes, and special purpose processing nodes. Intended to provide highly available, fast, and secured connections to any application or service from any authorized network at any time.
Software application rationalization and server virtualization	An effort intended to enable IT efficiencies and enhance information sharing.
Desktop virtualization and thin-client environment	A standardized virtual desktop environment intended to achieve IT efficiencies and allow users to access their computing environments from any thin client[a] or mobile device, from any DOD location.
Mobility services	Integration of secure and non-secure communications and portable, cloud-enabled command and control capability to increase the number of people able to collaborate and share information rapidly.
Enterprise services	Services such as unified communications, IT applications, e-mail, and collaboration capabilities, provided in a common way across the department.
Mission partner environment	DOD plans to provide a common set of standards, protocols, and interfaces to enable secure, reliable sharing of data with a wide array of mission partners. The partners include other federal, state, and local agencies; allies; coalition partners; and private sector organizations. A gateway is planned to monitor and control this sharing.

Source: GAO analysis of DOD documentation. I GAO-16-593.

[a]A thin client is a computer or computer program that depends heavily on another computer to fulfill its traditional computational needs.

JIE is managed by an executive committee that is tri-chaired by the DOD Chief Information Officer (CIO), the Joint Staff CIO, and U.S. Cyber Command. More details about JIE governance and oversight are provided later in this report.

Joint Regional Security Stacks

According to the DOD CIO, the department is currently focused on implementing JRSS to enable the single security architecture. The effort, which is managed by the Defense Information Systems Agency (DISA), involves installing and implementing various hardware and software components, including

- "security stacks," which comprise network security devices that perform routing and security functions;
- a joint management system to provide centralized network management capability; and
- cyber situational awareness and analytic capability to enable situational awareness for strategic, regional, and local command and control activities.

JRSS is intended to enhance network command and control, increase bandwidth, and synchronize networks. It is to be used to screen network traffic to and from DOD installations, control traffic flows, identify and block unauthorized traffic, and isolate intrusions. To achieve these ends, JRSS is expected to replace about 1,000 non-standardized network security stacks, currently located across the globe, with 48 standardized stacks at 25 locations, reducing the number of avenues for cyber attack. Because each of the military departments' existing capabilities differ, DOD plans to deliver JRSS in three increments: 1.0 by the end of the first quarter of fiscal year 2017, 1.5 in the third quarter of fiscal year 2017, and 2.0 by the end of fiscal year 2019.

The department estimates that it will have spent over $900 million on JRSS in fiscal year 2013 through fiscal year 2016, and will spend approximately $1.6 billion more in fiscal years 2017 through 2021. More information about JRSS cost is provided later in this report.

Implementation Approach

The JIE implementation strategy states that JIE is not a program of record or an acquisition program.[5] A program of record, according to the

[5]DOD officials have stated that JIE is not a formal acquisition program, pursuant to DOD acquisition policy.

Defense Acquisition University,[6] is recorded in the department's Future Years Defense Program, which is an outcome of DOD's planning, programming, budgeting, and execution process. The purpose of the process is to allocate resources to programs within the department. An acquisition program, according to DOD policy,[7] is a directed, funded effort that provides a new, improved, or continuing information system or service capability, among other things, in response to an approved need.[8]

According to DOD officials, JIE is a construct for managing improvement and modernization of DOD's IT infrastructure and the associated operational concepts, and does not have a discrete beginning or ending such as would be expected with a program. Furthermore, according to the JIE implementation strategy, the department plans to use existing DOD component programs, initiatives, technical refresh plans, acquisition processes, and funding to deploy and migrate the existing infrastructure to JIE standards.

Leading Practices for Implementing Programs and Projects

The Project Management Institute describes a program as a means of executing a strategy and achieving organizational goals and objectives and states that programs include related projects and program activities.[9] The institute describes a project as an effort with a definite beginning and

[6]Department of Defense, Defense Acquisition University, *Glossary of Defense Acquisition Acronyms & Terms*, 16th Edition (Fort Belvoir, Va.: September 2015) and *Defense Acquisition Guidebook*, accessed August 19, 2015, https://acc.dau.mil/communitybrowser.aspx?id=488289

[7]Department of Defense Directive 5000.01, *The Defense Acquisition System*, (2003).

[8]Certain major DOD IT investments that are designated acquisition programs are governed by a statutory and regulatory oversight framework. Generally, under the framework, programs must, for example, meet requirements for establishing cost, schedule, and performance baselines and reporting on significant or critical variances. See, for example,10 U.S.C. §§ 2445a-2445c. See also Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015).

[9]Project Management Institute, Inc., *The Standard for Program Management –Third Edition* (Newtown Square, Pa: 2013). The Project Management Institute, Inc., founded in 1969, is a not-for-profit association that provides standards and guidance, which are used worldwide, on how to manage various aspects of projects, programs, and portfolios.

end that is intended to create a unique product, service, or result.[10] Entities such as the Project Management Institute, the Software Engineering Institute at Carnegie Mellon University, the National Institute of Standards and Technology, and we have developed and identified leading practices to help guide organizations to effectively plan and manage programs and projects such as JIE and JRSS. These practices include:

- Scope management: A program's scope represents the work required to deliver a benefit (major product, service, or result). A defined scope provides the context and framework for reporting, tracking, and controlling program activities. Scope management includes defining, assessing, and documenting the essential aspects that will be accomplished and developing a plan for managing, documenting, and communicating scope changes.
- Cost management: Cost management involves establishing a reliable cost estimate and baseline. A cost estimate is the summary of individual cost elements, using established methods and valid data, to estimate a program or project's expected cost. Managing a cost estimate involves documenting a cost baseline and analyzing differences between a cost baseline and actual costs.

Key implementation planning practices include:

- Schedule management: Schedule management involves establishing a reliable schedule and schedule baseline. Establishing a reliable schedule requires a program or project to identify the specific actions to be performed, their sequence and duration, resource requirements, and schedule constraints. To monitor and control the schedule, a program or project establishes a schedule baseline and the approved baseline dates are compared to actual start and finish dates to determine whether variances have occurred.
- Workforce planning: A strategic approach to workforce planning includes using data-driven, fact-based methods to document workforce needs and establish plans for addressing those needs. Among other things, workforce planning includes documenting and

[10]Project Management Institute, Inc.*, A Guide to the Project Management Body of Knowledge (PMBOK® Guide)—Fifth Edition* (Newtown Square, Pa: 2013). *PMBOK* is a trademark of Project Management Institute, Inc.

assessing the knowledge and skills needed to execute work roles; establishing an inventory of the knowledge and skills of current staff; conducting a gap analysis of the number of staff and the specific skills and abilities necessary to meet human capital needs; and establishing plans to address identified gaps.

- Security planning: System security planning is the process of planning adequate, cost-effective security protection for a system. Security planning involves providing an overview of the security requirements of the system and describing the controls in place or planned for meeting those requirements.

DOD Has Taken Steps to Implement JIE, but Needs to Improve Program Management and Planning

DOD has taken steps to implement JIE, but the department has not fully addressed key program management and planning practices. In particular, the department has not adequately defined the effort's scope or expected cost. In addition, DOD has not established a reliable schedule or sufficiently developed workforce and security assessment plans.

Officials provided a variety of reasons for the current status of JIE management and planning. For example, officials reported that assessing the cost of JIE is complex because of the size and the complexity of the department's infrastructure and JIE's implementation approach. To its credit, the department has an effort underway to improve its JIE management and planning, but the effort does not address all of the key processes that need to be improved, and time frames associated with this effort have not yet been established. As a result of the program's management and planning weaknesses, DOD decision makers and congressional stakeholders lack reliable information needed to make informed decisions about progress and needed changes.

Scope is Not Well Defined or Managed

According to the Project Management Institute,[11] program scope encompasses all the benefits (products and services) to be delivered by the program, and defines the work required to deliver a benefit. Effective program scope management includes developing a detailed program scope statement, which is verified and approved by stakeholders; breaking down the program work into deliverable components; and developing a plan for managing the scope throughout the program.

A scope statement helps provide the context and framework for reporting, tracking, and controlling the program. It is also needed to develop a program work breakdown structure that, in turn, is used to develop a reliable cost estimate and schedule. In addition, recognizing that scope and content are continually elaborated, clarified, and adjusted, a plan for managing, documenting, and communicating scope changes is necessary.

DOD has not effectively defined or managed JIE's scope. While the department has defined JIE scope at a high level, its scope is not sufficiently defined to determine what, specifically, is and is not included in JIE. For example, the 2013 JIE implementation strategy includes software application rationalization and desktop virtualization as part of JIE; however, briefings provided to congressional staff and to us[12] in 2015 did not specifically include this element. In addition, the briefings included other elements that were not specifically discussed in the implementation strategy. For example, in 2015, DOD CIO officials described JIE as including additional elements, such as Mission Partner Environment and Strategic Sourcing. However, the JIE implementation strategy has not been revised to document these additional elements. Furthermore, the department has not developed a plan for managing, documenting, and communicating JIE scope changes.

[11]Project Management Institute, Inc., *The Standard for Program Management – Third Edition*. Although DOD is not managing the JIE effort as a formal program of record or an acquisition program, the effort meets the Project Management Institute's definition of a program as a means of executing a strategy and achieving organizational goals and objectives and includes related projects and program activities. Accordingly, we assessed JIE as a program.

[12]DOD CIO, *Joint Information Environment Overview*, March 3, 2015 and Deputy CIO for Information Enterprise, *GAO Engagement on the Joint Information Environment*, July 24, 2015.

See table 2 for a list of elements described in the JIE implementation strategy and in 2015 briefings.

Table 2: JIE Elements as Described in Various DOD Sources

September 2013 implementation strategy	March 2015 DOD CIO presentation to congressional staff	July 2015 Deputy DOD CIO briefing to GAO
Single security architecture	Cyber security architecture	Cyber security architecture
Normalized federated networks	Network modernization	Network modernization
Data center consolidation	Data center consolidation	Data center consolidation
Identity and access management	Identity and access management	Identity and access management
Enterprise services	Enterprise services	Enterprise services
Software application rationalization and server virtualization		
Desktop virtualization and thin-client environments		
Mobility services	Mobility	Mobility
Cloud computing	Cloud computing	Cloud computing
	Mission partner environment	Mission partner environment
	Enterprise operations	Enterprise operations
		Computing environment
		Strategic sourcing

Source: GAO analysis of DOD documentation. I GAO-16-593.

According to DOD CIO officials, briefings to congressional staff are a way to formally document scope changes. However, the changes in scope that were briefed to congressional staff and to us were not documented in a verified and approved scope statement, and DOD has not updated its 2013 implementation strategy to reflect JIE scope changes.

With respect to establishing a plan for managing, documenting, and communicating scope, an official from the Office of the Deputy DOD CIO (Information Enterprise) explained that there are efforts underway to update the existing governance structure and processes. These efforts include identifying use cases for the decisions and processes needed to support JIE. For example, one of the proposed use cases is focused on the process for planning and approving deployment of new capabilities.

However, the use cases are still under development and none are specifically focused on managing scope changes. Moreover, as of March 2016, the department had not established a time frame for completing its efforts to update governance processes.

Without a current and approved program scope statement, DOD risks that stakeholders will not have a clear understanding of the work required to achieve the expected benefits. For example, Marine Corps officials told us that they were concerned that a strategy was not in place to lay out what is next beyond the Joint Regional Security Stacks. They also added that JIE is to include consolidation of applications and data into centralized data centers, but that it was not clear how this fits in with the overall strategy.

In addition, until a scope statement is verified and approved, DOD's ability to develop a work breakdown structure that could be used for establishing a reliable cost estimate is limited. Moreover, DOD lacks information needed by DOD officials and congressional committees to oversee progress, help ensure accountability for performance, and make more informed resource decisions. Finally, without a defined approach for managing scope, the department lacks a foundation for managing its scope and providing appropriate context and a framework for reporting, tracking, and controlling JIE-related activities.

DOD Has Not Estimated JIE Costs or Established a Reliable JRSS Cost Baseline

According to the Project Management Institute, effective program financial management includes integrating the budgets of program components (e.g., projects), developing an overall cost baseline, and monitoring and controlling program and project costs.[13] In addition, program cost estimating should be performed throughout the life cycle. For example, given the typically long duration of a program, initial estimates may need to be updated to reflect the current environment and cost considerations. The program budget should include the costs for each component as well as the resources to manage the program. Once a baseline budget has been established, it becomes the financial measure for the program.

[13]Project Management Institute, Inc., *The Standard for Program Management–Third Edition*, 2013.

Consistent with these practices, the *National Defense Authorization Act for Fiscal Year 2013* (NDAA) required DOD to develop a JIE implementation strategy that included, among other things, an assessment of the resources needed to achieve the JIE vision, including the anticipated implementation cost.[14] More recently, the Office of the Director, Operational Test and Evaluation, in its January 2016 report to Congress, recommended that the department improve its efforts to oversee JIE cost.[15]

DOD has not yet developed an estimate of the cost to implement JIE. According to the report DOD prepared in response to the NDAA for Fiscal Year 2013, assessing JIE life cycle costs is highly complex, given the size and complexity of the DOD infrastructure and JIE's implementation approach.[16] Nevertheless, the department also reported that it planned to assess JIE costs. Specifically, in March 2016, DOD CIO officials stated that cost estimates are being established as the department defines the specifics associated with elements of JIE.

As discussed previously in this report, DOD has efforts underway to update the existing governance structure and processes. These efforts include identifying use cases for the decisions and processes needed to support JIE, including determining the policy and process for reviewing and/or analyzing cost estimates. However, as of March 2016, the department had not established a time frame for completing its efforts to update governance processes.

Until DOD determines how it will document the costs of its JIE effort and officials and congressional committees are provided accurate information about expected costs, they are limited in their ability to provide oversight for performance and make effective resource decisions.

[14]*National Defense Authorization Act for Fiscal Year 2013*, Pub. L. No.112-239, § 931, 126 Stat. 1632, 1883 (Jan. 2, 2013).

[15]The Director, Operational Test & Evaluation is the principal staff assistant and senior advisor to the Secretary of Defense on operational test and evaluation. The Director is responsible for providing independent assessments on operational test and evaluation activities to Congress and the Secretary of Defense.

[16]*The Department of Defense Strategy for Implementing the Joint Information Environment*, 2013.

A Reliable Cost Baseline Does Not Exist for JIE's Primary Effort, JRSS

According to key project management practices, a project cost baseline is an approved summary of the estimated costs over the relevant time frame and is to be used as a basis for comparison to actual results.[17] The baseline can only be changed through formal change control procedures. Consistent with this practice, policy and guidance from DISA, which manages the JRSS effort, says all programs, projects, services, enterprise services, initiatives, and other acquisition-related matters, including technical refresh efforts, should have an approved cost baseline, and that the baseline is to be regularly evaluated against execution.[18] In addition, DISA policy states that cost estimates are to cover the entire life cycle. Further, it states that best practices are to be employed across the acquisition life cycle to the greatest extent practicable.

DISA's IT Acquisition Guide notes that cost estimates should follow a standardized process such as the one identified in our cost estimating and assessment guide.[19] In addition to providing steps to follow for developing a cost estimating process, our guide identifies four characteristics of a reliable cost estimate: well-documented, comprehensive, accurate, and credible.

DOD provided various estimates of JRSS costs, and in March 2016, the department approved a budget for JRSS for fiscal years 2017 through 2021. DOD officials described this budget as the JRSS cost baseline; however, the budget does not reflect the full estimated cost of JRSS. Specifically, it does not include about $900 million already spent on JRSS in fiscal years 2013 through 2016. According to the September 2015 cost estimate, the most recent available, JRSS was estimated to cost about $1.7 billion for fiscal years 2017 through 2021. The estimate, however, was not reliable. Table 3 contains our evaluation of DOD's September

[17]Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)—Fifth Edition*, 2013.

[18]Defense Information Systems Agency, *Information Services Acquisition Oversight and Management*, DISA Instruction 610-225-2 (Feb. 19, 2015) and *DISA IT Acquisition Guide: Proactively Tailored Acquisition Models and Processes to Guide DISA's Acquisition of IT Products and Services*, Version 1.0 (Nov. 1, 2013).

[19]GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009).

2015 JRSS cost estimate relative to the characteristics of a reliable cost estimate described in our cost estimating and assessment guide.[20]

Table 3: Assessment of the September 2015 JRSS Cost Estimate's Reliability

Characteristic	Description	Assessment	Description of assessment
Well documented	Estimates should be well documented. They should, among other things, state the purpose of the estimate and its scope; disclose key ground rules and assumptions, the estimating methodology and rationale, and the results of a risk analysis; and provide a conclusion about whether the cost estimate is reasonable. Finally, the cost estimates should be reviewed and accepted by management.	◐	The JRSS cost estimate is partially documented. DOD developed a JRSS cost estimate for fiscal years 2017 through 2021, which was used to support an approved budget request. The cost estimate included estimated costs for JRSS capabilities, including JRSS versions 1.5 and 2.0, joint management system versions 1.5 and 2.0, multiprotocol label switching, and cyber situational awareness analytic capability. However, DOD has not disclosed key ground rules and assumptions; documented the estimating methodology and rationale; or provided a conclusion about whether the cost estimate is reasonable.
Comprehensive	Estimates should include all costs over the program's full life cycle, from inception through operation and maintenance to retirement. They should also provide sufficient detail and reflect all cost-influencing ground rules and assumptions.	◐	The cost estimate is not fully comprehensive. The JRSS estimate identifies about $1.7 billion in investment, operations, and sustainment costs for fiscal years 2017 through 2021;[a] however, it does not include full life-cycle costs. Specifically, it does not include about $900 million already spent on JRSS 1.0 in fiscal years 2013 through 2016. In addition, though the September 2015 cost estimate includes some labor costs, such as labor costs for testing and migration, the November 2015 JRSS Implementation Plan states that the department had yet to determine the number of staff needed to complete migration to JRSS.
Accurate	Estimates should not be overly conservative or optimistic and should be, among other things, based on an assessment of the most likely costs. Also, the estimate should be grounded in documented assumptions that can be verified by supporting data and a historical record of actual cost and schedule experiences on comparable programs.	◐	DOD did not document information necessary to ensure the accuracy of its JRSS cost estimate. DOD officials stated that actual costs from comparable initiatives/contracts were used, and the cost estimate documentation identified the costs of products to support the cost estimate. However, the department did not document the assumptions or the steps used to develop its estimate.

[20]GAO-09-3SP.

Characteristic	Description	Assessment	Description of assessment
Credible	Estimates should discuss any limitations in the analysis due to uncertainty or biases surrounding the data and assumptions. Major assumptions should be varied and other outcomes computed to determine how sensitive the estimate is to changes in the assumptions. Risk and uncertainty inherent in the estimate should be assessed and disclosed. Further, the estimate should be properly verified by, for example, comparing it with an independent cost assessment.	○	The cost estimate is not credible. DOD did not assess or disclose risk or uncertainty in its estimate, such as the lack of finalized JRSS 2.0 functional requirements,[b] implementation plans, and workforce requirements. In addition, though CIO officials stated that DOD's Cost Assessment and Program Evaluation office[c] had reviewed the estimated costs in the JRSS funding request for fiscal year 2017 and beyond, officials said that they did not verify the estimated costs because they serve in an advisory capacity for JIE and JRSS and were not requested to verify the costs.

Legend: Fully satisfied criteria ● Met some, but not all, of the criteria ◐ Did not satisfy criteria ○

Source: GAO analysis of agency data. I GAO-16-593.

[a]In March 2016, DOD approved a JRSS budget of $1.6 billion for fiscal years 2017 through 2021.

[b]According to DOD, the JRSS 2.0 Functional Requirements Document was approved on May 9, 2016.

[c]According to the DOD Directive, *Director, Cost Assessment and Program Evaluation* (Number 5105.84), May 11, 2012, the Director is the principal official for independent cost estimation and cost analysis, and ensuring that the cost estimation and cost analysis processes provide accurate information and realistic estimates of cost for DOD's acquisition programs. In addition, the JIE Management Construct calls for the Cost Assessment and Program Evaluation Office to provide the overall department-level analytical framework for evaluating plans, programs, and budgets through the department's planning, programming, budgeting, and execution processes.

DOD officials disagreed with our assessment of the JRSS cost estimate. In particular, they stated that the cost estimate is adequate and that it supported an approved budget request. With respect to not including the amount that will have been spent on JRSS in fiscal years 2013 through 2016 in the cost estimate, DOD CIO officials said that the prior year funds were previously programmed for military department-specific approaches and were realigned to deliver enterprise-wide modernization of JRSS. However, without an estimate of the full cost of JRSS, DOD officials and congressional stakeholders will not have the information needed to help ensure accountability for project performance relative to predefined cost expectations for the effort as a whole, and make informed decisions about limited DOD and federal government resources.

DOD CIO officials also stated that an independent cost assessment is not planned because JRSS is commercial off-the-shelf equipment that will refresh existing technology, not new technology. Nonetheless, considering that the department estimated JRSS to cost $1.7 billion in fiscal years 2017 through 2021, an independent review of the cost estimate's quality and reliability would help ensure that the estimate used

to support the budget decision is valid.[21] Moreover, although DOD considers JRSS to be a technical refresh effort and not an acquisition program, JRSS meets the cost thresholds to be defined as a major automated information system program. Accordingly, if the department chose to designate it as such a program, an independent cost estimate would be required.[22]

Implementation Planning Needs to be Improved

According to leading schedule management practices, programs and projects should have baseline schedules that have been approved by stakeholders and are used to keep the program on track.[23] A program schedule should include the milestones to be measured and both program-unique activities and the projects that will deliver the program scope. In addition, a baseline schedule provides a basis for comparing actual start and finish dates with baseline dates to determine whether variances have occurred, and the baseline can only be changed through formal change control procedures. Moreover, a schedule management plan should be developed to provide guidance and direction on how the schedule will be managed. Specifically, the schedule management plan

[21]See GAO-09-3SP for eight types of independent cost estimate reviews.

[22]10 U.S.C. § 2445a defines major automated information system programs and specifies cost thresholds for designation as a major automated information system. As implemented by DOD, an automated information system acquisition is categorized as a major acquisition if spending is estimated to exceed certain thresholds, for example, $165 million in fiscal year 2014 constant dollars for all expenditures for all increments, regardless of the appropriation or fund source, directly related to the program's definition, design, development and deployment, beginning from the material solution analysis phase through deployment at all sites. DOD further defines an automated information system as a system of computer hardware, computer software, data or telecommunications that performs functions such as collecting, processing, storing, transmitting, and displaying information. One of the exclusions from this definition is computer resources, both hardware and software, that are determined to be better overseen as a non-automated information system program (e.g., a program with a low ratio of research, development, test and evaluation funding to total program acquisition costs or that requires significant hardware development). Officials responsible for major automated information system programs are required to prepare an independent cost estimate for milestone decision authority approval at certain acquisition milestones. Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 15, 2015).

[23]Project Management Institute, Inc. *The Standard for Program Management—Third Edition* and *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)—Fifth Edition,* 2013. Also, see GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: December 2015).

should establish the criteria and procedures needed to develop, change, monitor, and control the schedule.

Consistent with this practice and similar to DISA's policy and guidance for a cost baseline for all programs, projects, services, enterprise services, initiatives, and other acquisition-related matters, including technical refresh efforts, DISA policy and guidance says an approved schedule baseline should be established, and that the baseline should be regularly evaluated against execution.[24] Further, DISA policy states that best practices are to be employed across the acquisition life cycle to the greatest extent practicable. Moreover, the Office of the Director, Operational Test and Evaluation,[25] in its January 2016 report to Congress, recommended that the department improve its efforts to oversee the JIE schedule.

DOD has not defined an end date or key milestones associated with the overall JIE effort. With respect to the JRSS component of JIE, according to the November 2015 JRSS Implementation Plan, senior department leadership directed JRSS implementation by the end of fiscal year 2019. As of November 2015, the department planned to complete installation of 1.0 by the end of the first quarter of fiscal year 2017. DOD plans to complete installation of 1.5 in the third quarter of fiscal year 2017.

To support its planning and management efforts, DOD has developed integrated master schedules for JIE and JRSS and updates them periodically. However, the department has not established reliable schedule baselines to serve as the basis for comparing actual progress versus expected progress to measure program and project performance. Instead, DOD officials from DOD CIO and DISA stated that the department makes changes to the schedules on an as-needed basis;

[24]Defense Information Systems Agency, *Information Services Acquisition Oversight and Management*, DISA Instruction 610-225-2 (Feb. 19, 2015) and *DISA IT Acquisition Guide: Proactively Tailored Acquisition Models and Processes to Guide DISA's Acquisition of IT Products and Services*, Version 1.0 (Nov. 1, 2013).

[25]The Director, Operational Test & Evaluation is the principal staff assistant and senior advisor to the Secretary of Defense on operational test and evaluation. The Director is responsible for providing independent assessments on operational test and evaluation activities to Congress and the Secretary of Defense.

however, the department has not established criteria and procedures for approving changes to the schedules.

Without a documented, consistently applied schedule change control process, program staff can continually revise the schedule to match performance, hindering management's insight into the true performance of the program and project. Accordingly, unless DOD defines and follows procedures for updating the schedules, DOD management and congressional stakeholders will lack complete insight into schedule changes, thus limiting accountability for performance relative to expected baselines.

Schedules are Unreliable

Our schedule assessment guide includes best practices for developing high-quality, reliable schedules.[26] These practices include

- capturing all activities,
- assigning resources to activities,
- conducting a schedule risk analysis, and
- confirming that a critical path is valid.

DOD has developed integrated master schedules for both JIE and JRSS, and uses them to provide updates to senior leaders. However, the schedules do not address key aspects of reliable schedules. For example, they do not include certain key activities, reflect needed resources, or identify a critical path. See table 4 for our evaluation of DOD's JIE and JRSS schedules.

[26] GAO-16-89G.

Table 4: Assessment of the JIE and JRSS Integrated Master Schedules (IMS)

Practice	Description	Assessment of JIE IMS	Assessment of JRSS IMS
Capturing all activities	An IMS should reflect all activities necessary to accomplish a program or project's objectives. The schedule should reflect all activities defined in a work breakdown structure, which should reflect the program's scope.	The JIE IMS does not include all key activities. For example, the IMS does not include security assessments that are required by Execute Orders.[a]	The JRSS schedule does not include all key activities. For example, the IMS does not include steps that are planned to address security-related activities, such as implementation sites obtaining an authorization to operate in accordance with the department's new risk management framework, and activities related to obtaining cyber situational awareness and analytic capability.
Assigning resources to activities	The IMS should reflect the resources (e.g., labor) needed to do the work, whether they will be available when needed, and any funding or time constraints.	JIE's IMS assigns responsibility for activities to DOD entities, such as the DOD CIO and DISA. However, it does not reflect the resources needed to complete activities and whether they will be available when needed.	The JRSS schedule does not reflect resources needed to do the work and whether they will be available when needed.
Conducting a schedule risk analysis	A schedule risk analysis should be conducted to identify high-priority risks and steps to mitigate them.	DOD has not conducted a JIE schedule risk analysis.	DOD has not conducted a JRSS schedule risk analysis.
Confirming that a critical path is valid	The schedule should identify the critical path—the path of longest duration through the sequence of activities. Establishing a valid critical path is necessary for examining the effects of any activity slipping along this path. The critical path determines the earliest completion date and focuses the team and management on the activities that will lead to the program's success.	The JIE IMS does not identify a critical path.	The JIE Executive Committee has been briefed on the critical path of some portions of JRSS. For example, in September 2015, the committee was briefed on the critical path of some JRSS 1.0 activities. However, the JRSS IMS does not have a valid critical path. Specifically, it does not identify a continuous path to major completion milestones.

Source: GAO analysis of agency data I GAO-16-593.

[a]In December 2012, the Joint Staff issued a JIE Execute Order, which requires U.S. Cyber Command, in coordination with the Combatant Commands, to conduct a security assessment of JIE incremental plans. In September 2013, the Joint Staff added a requirement to the order for the National Security Agency to conduct a security impact assessment of the JIE security architecture.

A DOD CIO official responsible for managing the JIE IMS stated that it is not a typical IMS. Instead, according to the official, the schedule is a compilation of projects and initiatives and is sufficient to provide DOD managers with a tool to identify discrepancies and schedule risks, monitor

execution, and inform stakeholders to make decisions. However, without a reliable schedule or clear insight into a critical path, DOD cannot reliably determine the impact that changes to individual activities will have on other related efforts. This is particularly important due to the many different efforts associated with JIE.

DOD CIO officials stated that some of the issues we identified with the JRSS IMS are addressed by other means. For example, with respect to schedule resources, these officials stated that DISA has determined a standard number of resources (i.e., the number of persons and duration) needed to install and configure each security stack. They added that they recognized there will be fluctuations based on the unique requirements at each installation. However, unless the schedule includes information about schedule resources, officials are less able to determine the impact of fluctuations in resource needs on the overall schedule. In addition, without addressing other practices, such as including a critical path, the department's ability to determine the impact of changes, such as these fluctuations, is further limited.

The Office of the Director, Operational Test and Evaluation, noted in its January 2016 report that a lack of overall schedule discipline has contributed to the delay in an early operational assessment that was originally planned for March 2014 and is currently planned for the fourth quarter of fiscal year 2016 or later. Accordingly, the office recommended that the department take steps to improve its efforts to oversee the JIE schedule.

As discussed previously, DOD has an effort underway to update the existing JIE governance structure and processes. However, this effort does not currently include improving schedule management as a process that will be addressed. Until DOD documents how the JIE and JRSS schedules are to be managed, and improves how it manages them, DOD officials and congressional stakeholders will not have reliable information needed to identify schedule risks, monitor execution, and make well-informed decisions about the efforts.

Strategic Workforce Planning Needs to be Improved

We have previously identified key practices for effective strategic workforce planning.[27] These practices include

- assessing the knowledge and skills needed to execute a program;
- inventorying the knowledge and skills of existing staff;
- forecasting the knowledge and skills needed over time;
- analyzing the gaps in capabilities between the existing staff and future workforce needs, including consideration of evolving program and succession needs caused by turnover and retirement; and
- formulating strategies for filling expected gaps.

Consistent with these key practices, DOD's *Initial Capabilities Document for Joint Information Environment,* published in July 2014, requires DOD to develop department-wide knowledge, skills, and certification requirements that can be implemented across all components.[28] Specifically, it says that, due to the operationalization of JIE capabilities at a joint level, standardized workforce competencies will be integral to the realization of JIE. It also requires each DOD component to review personnel issues to ensure appropriate skill sets are available to employ JIE capabilities. Further, the document notes that, while JIE should not result in a net increase in required manpower, the types of skill sets and collocation of those skill sets into regional and global centers will require careful personnel management.

Furthermore, the NDAA for fiscal year 2013 required the department to develop a department-wide personnel plan for making JIE operational.[29] The law required the plan to include a validated Joint Staff requirement for manpower levels and the levels required for each of the military departments and combat support agencies needed for full spectrum cyber

[27]GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003). See also GAO, *DOD Business Systems Modernization: Further Actions Needed to Address Challenges and Improve Accountability*, GAO-13-557 (Washington, D.C.: May 17, 2013).

[28]The *Initial Capabilities Document* is intended to define the broad capabilities required to effectively, efficiently, and securely operate DOD's global IT infrastructure and provide access to required information at the point of need.

[29]*National Defense Authorization Act for Fiscal Year 2013*, Pub. L. No. 112-239, § 931(b) 126 Stat. 1883.

operations, including the national cyber defense mission and the operational plans of the combatant commands for each fiscal year across the current future-years defense program.[30]

The department has taken steps to identify the workforce needed to realize JIE and develop department-wide knowledge, skills, and certification requirements that can be implemented across all components. Specifically, the department has begun to document and assess the knowledge and skills needed to execute cyber work roles, including for JIE; however, it still needs to inventory the knowledge and skills of current staff, and perform a gap analysis of the number of staff and the specific skills and abilities needed to effectively achieve the JIE vision. See table 5 for our evaluation of workforce planning.

Table 5: Assessment of JIE Strategic Workforce Planning

Practice	Rating	Assessment
Assess the knowledge and skills needed to execute a program	◐	The department has begun to assess the knowledge and skills needed to execute JIE. According to the March 2014 JIE Personnel Plan, the department plans to develop and document the knowledge, skills, and abilities required for JIE. Specifically, according to the plan, the department's DOD Cyberspace Workforce Framework will define the department-wide cyberspace workforce and the work it performs, and relevant work roles in support of JIE will be identified predominantly from the roles of the IT and cybersecurity workforces. The department has developed the draft Cyberspace Workforce Framework, which defines workforce roles, by category and specialty area, and includes the underlying knowledge, skills, and abilities required of personnel performing the work and the tasks to be performed. According to DOD CIO officials, more work is underway to further develop and refine the framework. Specifically, according to officials, working groups were to be established in April 2016 to complete the qualification requirements for individual work roles. For example, these qualification requirements include, among other things, education, training, residency, credentials, and continuous development. In addition, the personnel plan notes that until other planning aspects of JIE are complete, the requirements for the personnel roles cannot be fully developed and validated.
Inventory knowledge and skills of existing staff	○	The department has yet to inventory knowledge and skills of existing staff. Specifically, it has yet to finalize its Cyberspace Workforce Framework, which is to be used to identify the relevant work roles and the underlying knowledge and skills for JIE.

[30]DOD's future-years defense program is the department's financial plan over a 6-year period.

Practice	Rating	Assessment
Forecast the knowledge and skills needed over time	◐	The department has begun to forecast the knowledge and skills needed over time for JIE. Specifically, it has developed the DOD Cyberspace Workforce Framework that documents the knowledge, skills, and abilities required for cyber work roles, including those necessary for JIE. However, according to DOD CIO officials, more work is underway to further develop and refine the framework. Specifically, according to officials, working groups were to be established to complete the qualification requirements for individual work roles. For example, these qualification requirements include, among other things, education, training, residency, credentials, and continuous development.
Analyze the gaps in capabilities between the existing staff and future workforce needs, including consideration of evolving program and succession needs caused by turnover and retirement	○	The department has yet to analyze the gaps in capabilities between the existing staff and future workforce needs for JIE. Although the department has documented work roles for its cybersecurity workforce in its DOD Cyberspace Workforce Framework, it has not yet leveraged the framework to inventory department-wide knowledge and skills of existing staff or analyze the gaps in capabilities between the existing staff and future workforce needs.
Formulate strategies for filling expected gaps	○	In December 2013, the department developed a Cyberspace Workforce Strategy, which includes focus areas for building and maintaining a competent and resilient cyberspace workforce. For example, the strategy includes establishing a cohesive set of DOD-wide cyberspace workforce management issuances, including the Cyberspace Workforce Framework. However, the department has not yet identified gaps, thus it has not formulated strategies for filling expected gaps.

Source: GAO analysis of DOD documentation. I GAO-16-593.

Furthermore, although the department developed the JIE Personnel Plan, it has yet to address the Fiscal Year 2013 NDAA requirement for documenting a validated Joint Staff requirement for manpower levels for making JIE operational. DOD CIO officials stated that it is the military departments' responsibility to determine their manpower needs and the department does not plan to update the JIE Personnel Plan. Nevertheless, the NDAA calls for a department-wide personnel plan.

Without a clear understanding of JIE workforce needs, the department risks not being able to reliably ensure that it will have the appropriate workforce knowledge and skills needed over time to support JIE. In addition, the lack of a clear understanding of JIE workforce needs will limit the department's ability to reliably determine JIE-related costs.

DOD Lacks a Strategy to Conduct Required JIE Security Assessments

According to National Institute of Standards and Technology guidance,[31] a security impact assessment should be conducted to determine the extent to which proposed or actual changes to an information system or its environment can affect the security state of the system. The guidance also notes that a security impact assessment should be conducted prior to making changes to an information system or its environment.

Accordingly, the Joint Staff issued orders to conduct JIE security assessments. Specifically, in December 2012, the Joint Staff issued an Execute Order[32] that required the U.S. Cyber Command, in coordination with the combatant commands, to conduct a security assessment of JIE incremental plans.[33] In September 2013, the Joint Staff added a requirement to the order stating that the National Security Agency should conduct a security impact assessment of the JIE security architecture.[34]

In addition, in August 2014, the DOD Director of Operational Test and Evaluation issued procedures for programs under its oversight, which include JIE, to develop and submit a cybersecurity test and evaluation strategy for its review and approval, as part of their test and evaluation master plans.[35] According to these procedures, the strategy is to include

[31]National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems* Special Publication 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

[32]An Execute Order is typically an order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to initiate military operations. The purpose of the JIE order was to promulgate direction by the Secretary of Defense that the DOD CIO, Director of the Joint Staff, and Commander of Cyber Command provide JIE transformation planning, coordination, and execution, in conjunction with the combatant commands, services, and agencies throughout the Department of Defense.

[33]A security assessment can, for example, evaluate security controls (i.e., prescribed safeguards or countermeasures) to determine the extent to which they are properly designed, developed, implemented, and operating as intended. See National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems*.

[34]JIE Execute Order Modification-1 was issued September 12, 2013, to modify the original execute order. Modifications include the terms “No Change,” “Change to Read,” followed by a revision, or “Add,” followed by a new task.

[35]Department of Defense, Director, Operational Test and Evaluation, *Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs*, August 1, 2014.

information on network architecture, external network connections, the intended operational environment, and the anticipated cyber threat. The strategy should also describe, among other things, the resources needed to execute the strategy, responsible organizations, and a schedule of when the testing is to occur.

The Office of the DOD CIO established a team to review the JIE security architecture; however, DOD has not documented plans to complete the assessments. Specifically, the office established a joint team that includes U.S. Cyber Command and the National Security Agency, which has taken steps to conduct a review of the JIE security architecture. These steps included developing a threat framework and assessing security capabilities against adversary tactics, techniques, and procedures, and developing an interim report. However, DOD CIO officials said that the team has not documented plans for completing the security assessments because testing and assessments are the purview of the Director, Operational Test and Evaluation and the Joint Interoperability Test Command. DOD CIO officials added that the team was working with its sponsors to determine where it should concentrate its limited resources to provide the best information for decision makers. In a letter provided after our report was published, the Director, Operational Test and Evaluation, stated that the preparation of plans for JIE testing and assessments is the responsibility of the DOD CIO and the Defense Information Systems Agency, and that the Director, Operational Test and Evaluation, approves test plans and oversees operational test and evaluations for DOD. The Director added that JIE leadership has yet to adopt a test strategy. We did not assess which entity within DOD was responsible for planning for JIE security assessments. However, regardless of which entity is responsible, it is important that the department plan for and complete the assessments.

In addition, the department has yet to develop a JIE cyber security test and evaluation strategy. According to an official from the Office of the Director of Operational Test and Evaluation, as of April 2016, the department was in the process of developing an overarching test strategy.

Without a security assessment of JIE or a plan to conduct an assessment, DOD is limited in its ability to ensure security-related weaknesses and deficiencies are detected early so that cost-effective corrective measures for any identified weaknesses and deficiencies can be identified. Further, DOD is limited in its ability to identify security weaknesses and deficiencies that could potentially be inherited by lower-

level systems through common controls and cybersecurity reciprocity. Moreover, the lack of a security impact assessment hinders DOD from achieving key goals, such as ensuring increased cyber security through JIE.

Plan to Transition JRSS to New Security Risk Management Requirements Is Needed

Guidance published by the National Institute of Standards and Technology calls for agencies to use a risk management approach to building information security capabilities into federal systems, and provides a six-step risk management framework.[36]

Accordingly, DOD developed guidance that requires systems to transition to the risk management framework.[37] For a system to be authorized to operate in accordance with the guidance, DOD calls for those responsible for the system to (1) establish a security plan that includes an overview of the system's security requirements and describes the security controls in place or planned for meeting those requirements; implementation status; responsible entities; resources; and estimated completion dates and (2) develop a strategy and schedule for transitioning to the risk management framework and obtain authorizing official approval of the strategy and schedule.

DOD specified a set of JRSS security controls, in accordance with the requirements of its current authorization to operate. However, the department has yet to develop a JRSS security plan in accordance with DOD's new risk management framework, because it has not yet transitioned to the framework.

DOD drafted a plan to receive a risk management framework authorization to operate by March 2016. However, the transition has been delayed, and in March 2016, its current authorization to operate was extended until September 2016. The DISA official responsible for JRSS implementation said that transition to the risk management framework cannot occur until facilities where JRSS is to be installed receive their risk management framework authorizations to operate.

[36]National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems,* 2010.

[37]DOD Instruction on *Risk Management Framework for DOD Information Technology* (8510.01), March 12, 2014.

In addition, DOD has not updated its plan for transitioning to the risk management framework. According to the DISA official, a plan is not needed because the work is complete. However, work required to achieve an authorization to operate remains at JRSS installation sites.

Without a current security plan that identifies the JRSS security requirements and the security controls in place or planned for meeting those requirements, the department risks having a deficient security posture. Furthermore, without an approved strategy or schedule to authorize JRSS to operate in accordance with the new risk management standards, the department risks delaying JRSS implementation.

Governance and Oversight Can Be Strengthened

In November 2012, the department established the JIE Management Construct to manage and oversee JIE. The construct includes, primarily, an executive committee supported by a subordinate planning and coordination entity, called the Planning and Coordination Cell. Both of these entities are led jointly by DOD CIO, Joint Staff CIO, and U.S. Cyber Command. The construct describes the DOD CIO as the governance lead, U.S. Cyber Command as the operational sponsor, and the Joint Technical Synchronization Office, led by DISA, as the technical and implementation lead. Table 6 includes a description of key JIE Management Construct entities and their roles and responsibilities.

Table 6: Key JIE Management Construct Entities' Roles and Responsibilities

JIE Management Construct Entity	Description
JIE Executive Committee	Led jointly by the DOD CIO, Joint Staff CIO, and U.S. Cyber Command. Includes representatives from the Departments of the Air Force, Army, and Navy; the U.S. Navy and the U.S. Marine Corps; the Undersecretary of Defense (Acquisition, Technology and Logistics); Undersecretary of Defense (Intelligence); Undersecretary of Defense (Comptroller); Undersecretary of Defense (Personnel and Readiness); Director, Cost Assessment and Program Evaluation; the Deputy Chief Management Officer; and the combatant commands (e.g., European Command and Pacific Command). Responsible for setting the direction for JIE; establishing goals and objectives; providing oversight; and maintaining accountability. It develops plans, policies, and governance approaches; initiates reviews of programs, initiatives, and systems that it considers essential for enterprise-wide solutions and operational effectiveness; provides JIE standards; recommends investments; and enforces compliance. Provides decisions on the JIE execution plan, but may elevate issues to appropriate bodies, such as the Joint Chiefs of Staff Operational Deputies, the Deputy's Management Action Group, or the Undersecretary of Defense (Acquisition, Technology and Logistics) for decisions.

JIE Management Construct Entity	Description
JIE Planning and Coordination Cell	Led jointly by the DOD CIO, Joint Staff CIO, and U.S. Cyber Command, and includes the same members as the Executive Committee. Responsible for synchronizing DOD components' actions, maintaining the JIE integrated master schedule, tracking implementation plans, coordinating activities among governance, operations, and the JIE Technical Synchronization Office; and managing the resolution of implementation issues.
DOD CIO	Serves as tri-chair to the JIE Executive Committee and as the JIE governance lead. Responsible for aligning JIE to the department's requirements, budgeting, and acquisition processes. Provides overarching plans, guidance, and policy that inform requirements approval and development of the JIE enterprise architecture.
U.S. Cyber Command	Serves as the JIE operational sponsor. Responsible for developing, integrating, and synchronizing JIE operational tasks and procedures with existing department-level procedures. Works closely with the combatant commands and coordinates and leads the development of the operational concepts of operations and JIE tactics, techniques, and procedures.
JIE Technical Synchronization Office	Part of DISA; serves as the JIE technical and implementation lead. Responsible for developing, integrating, and synchronizing JIE technical plans, programs, and capabilities.
Combatant Commands	Theater-level sponsors for JIE implementation. Responsible for establishing a theater-level governance structure to synchronize and integrate theater-level actions necessary to deliver JIE.
DOD components	Responsible for implementing the tasks necessary to execute JIE plans.

Source: GAO analysis of the DOD documentation I GAO-16-593.

The JIE Executive Committee meets every two weeks to discuss JIE and JRSS activities and assigns and tracks action items. However, it does not monitor performance and progress relative to reliable cost and schedule baselines. See table 7 for our evaluation of JIE and JRSS governance.

According to leading governance practices,[38] to ensure effective program oversight, organizations should

[38]Project Management Institute, Inc., *The Standard for Program Management–Third Edition,* 2013; Software Engineering Institute/Carnegie Mellon, *Capability Maturity Model® Integration (CMMI®) for Development*, Version 1.3, CMU/SEI-2010-TR-033 (Hanscomb AFB, Massachusetts: November 2010) and *CMMI® for Acquisition*, Version 1.3, CMU/SEI-2010-TR-032 (Pittsburgh, Pa.: November 2010); and GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004). See also GAO, *Immigration Benefits System: Better Informed Decision Making Needed on Transformation Program*, GAO-15-415 (Washington, D.C.: May 2015).

- monitor program performance and progress toward expected cost, schedule, and benefits;
- ensure that corrective actions are identified and assigned to the appropriate parties at the first sign of cost, schedule, and/or performance slippages;
- ensure that corrective actions are tracked until the desired outcomes are achieved;
- use complete and accurate data to review program performance against expectations; and
- document policies and procedures for program governance and oversight.

Table 7: Evaluation of Governance and Oversight

Practice	Description	Summary
The governance board should monitor program performance and progress toward expected cost, schedule, and benefits.	This practice involves comparing actual values with estimates in the plan, and identifying significant deviations. Reviews are conducted at predetermined checkpoints and/or milestones, in order to interpret the data on project cost and schedule with respect to historic project data and expectations.	The Executive Committee meets every two weeks to discuss JIE activities. However, it does not monitor performance and progress relative to reliable cost and schedule baselines. In addition, the department has established operational metrics to assess outcomes (e.g., benefits) as JIE is implemented across the enterprise. However, the documentation containing the metrics notes that not all elements have evolved enough to define the measures and to enable reporting. Furthermore, the department has not established checkpoints or milestones for JIE.
The governance board should ensure that corrective actions are identified and assigned to the appropriate parties at the first sign of cost, schedule, and/or performance slippages.	This practice involves collecting and analyzing issues and determining corrective actions to address them. A corrective action is intended to realign program performance with the program plan.	The JIE Executive Committee identifies and assigns action items. However, these actions are not based on deviations from predefined cost and schedule expectations.
The governance board should ensure that corrective actions are tracked until the desired outcomes are achieved.	This practice involves regularly tracking the implementation of corrective actions until the actions are completed.	The JIE Executive Committee assigns and tracks action items. However, the actions are not based on predefined cost and schedule expectations. Moreover, some actions have remained open for lengthy periods of time. For example, in July 2015, the Executive Committee identified an action assigned to the JRSS Program Management Office to provide a schedule view showing the critical path of Joint Management System global deployment. The action item was due in August 2015. The due date has been extended several times, but as of February 2016, the action was past due.

Practice	Description	Summary
The governance board should use complete and accurate data to review program performance against expectations.	This practice involves relying on complete and accurate data to review program performance against stated expectations.	The JIE Executive Committee does not have complete and reliable cost and schedule data, as discussed elsewhere in this report. For example, JIE does not have a cost estimate. In addition, the JRSS cost estimate does not include complete workforce-related costs. With respect to schedule, the JIE and JRSS integrated master schedules do not identify key security-related activities.
The organization should document policies and procedures for program governance and oversight	This practice involves specifying policy and procedures for the governance board's oversight and operation, including reporting and control processes. Reporting and control processes may include, among others, operational status and progress of component projects and related activities; expected or incurred program resource requirements; known risks, risk response plans, and escalation criteria; benefits realized; decision criteria, tracking and communication; program funding and financial performance; threshold criteria to use when analyzing performance; and the conditions under which the project would be terminated.	The department established a JIE Executive Committee in 2012. Executive Committee members were identified and given roles and responsibilities. However, it has not established procedures for how reporting and controlling JIE should occur.

Source: GAO analysis of DOD data. I GAO-16-593.

Officials from the office of the DOD CIO disagreed with our assessment of governance. Specifically, they stated that JIE is a framework comprised of multiple elements and that each element has its own cost and schedule. These officials stated that when cost and schedule issues arise, they are briefed to the Executive Committee along with actions being taken to address them. For example, they stated that the manager responsible for JRSS implementation regularly briefs the Executive Committee on the status of JRSS, and the committee provides guidance and requires corrective action. However, as discussed previously in this report, the department does not have reliable JIE and JRSS cost and schedule baselines against which to compare updates to ensure that the effort is proceeding as expected.

A DOD CIO official explained that there are plans to update the existing governance structure and processes. The JIE integrated master schedule also includes plans to update governance processes. These plans include identifying use cases for the decisions and processes needed to support JIE. For example, one proposed use case is focused on determining how governance is to be linked to the department's decision processes, including programming, budgeting, and acquisition. However, the use

cases are still under development, and as of March 2016, the JIE integrated master schedule has not been updated to reflect the time frame for updating the governance structure and processes.

Until the Executive Committee further documents how cost, schedule, and performance of JIE and its related efforts are to be managed and bases its reviews of cost, schedule, and performance on complete and accurate data, the committee's ability to make timely, well-informed decisions and to provide effective oversight will be limited.

Conclusions

Given ongoing concerns about cyber security, as well as DOD's vast IT infrastructure and $38 billion IT budget, it is important that the department succeed in its efforts to achieve the JIE vision. While the department has established an executive committee to govern and oversee JIE, it lacks reliable scope, cost, and schedule information needed to effectively inform its efforts. The department has begun an effort to document its approach for improving JIE governance, but this effort is in its early stages.

In addition, DOD has begun to plan for JIE human capital needs, but further steps are needed to reliably ensure that it will have the appropriate workforce knowledge and skills needed over time to support JIE. Moreover, the department has taken steps to help ensure its JIE and JRSS efforts meet key security planning requirements, but more remains to be accomplished. In particular, without a complete JIE cyber security test and evaluation strategy or a strategy and schedule for transitioning JRSS to the new security risk management requirements, DOD risks having a deficient security posture due to not meeting key security-related goals or standards.

Furthermore, with respect to JIE governance and oversight, the JIE Executive Committee's efforts will not be fully effective until the department takes steps to ensure that its decisions are based on reliable scope, cost, and schedule information.

Recommendations for Executive Action

To help the department achieve the benefits anticipated from JIE, we are making nine recommendations to the Secretary of Defense. Specifically, we recommend that the Secretary direct the DOD CIO and other entities, as appropriate, to

- develop a detailed JIE scope statement that is verified by stakeholders and approved by the Executive Committee;
- establish a plan for managing, documenting, and communicating scope;
- develop a reliable JIE cost estimate and baseline, consistent with the best practices described in this report;
- develop a reliable JRSS cost estimate and baseline, consistent with practices described in this report;
- develop a JIE schedule management plan and reliable schedule, consistent with practices described in this report;
- develop a JRSS schedule management plan and reliable JRSS schedule and schedule baseline, consistent with practices described in this report;
- complete an assessment to determine the number of staff and the specific skills and abilities needed to effectively achieve JIE, consistent with the workforce planning practices described in this report;
- develop a strategy for conducting JIE security assessments that describes the resources needed to execute the strategy, responsible organizations, and a schedule to complete the assessments; and
- develop a strategy and schedule to transition JRSS to the Risk Management Framework, and develop the security plan required by the new framework.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from DOD. The comments are reprinted in appendix II.

In the comments, the department stated that it partially concurs with each of the recommendations and that the recommendations in the draft report will be applied where fiscally and technically feasible. DOD stated that its partial concurrence was due to the language we used to introduce the recommendations. Specifically, we stated that the Secretary of Defense should direct the appropriate entities to implement the recommendations. In its comments DOD stated that the DOD CIO is responsible for implementing JIE, and referred to a May 2013 memo from the Deputy Secretary of Defense directing DOD components to participate in and implement JIE under the direction of the DOD CIO.

In response to DOD's comments we revised the language used to introduce our recommendations. We are now calling for the Secretary to direct the DOD CIO and other entities, as appropriate, to take the recommended actions. The updated language more clearly recognizes the DOD CIO's role in directing JIE under the May 2013 memo. However, we retained the reference to other entities because the DOD CIO does not have direct authority over all important entities involved with JIE. For example, the JIE Executive Committee, which is charged with setting the direction for JIE, establishing goals and objectives, providing oversight, and maintaining accountability, is tri-chaired by the DOD CIO, the Joint Staff CIO, and U.S. Cyber Command. In addition, unlike other major federal agencies, the DOD CIO does not have budget request approval authority over DOD IT acquisitions across the department.[39]

The department also described steps it is taking or plans to take to address our recommendations. For four of the recommendations, the steps the department described will likely be sufficient if they are effectively implemented. For example, for the two recommendations aimed at developing a detailed JIE scope statement and a plan for managing, documenting, and communicating JIE scope, DOD stated that the DOD CIO intends to complete an updated JIE scoping document for stakeholder review and Executive Committee approval by December 2016. According to DOD, the new document will enable reporting, tracking, and controlling the department's IT modernization efforts. In addition, the department stated that the document will specify a process for communicating JIE scope updates.

Similarly, regarding our recommendation that DOD determine the number of staff and the specific skills and abilities needed to effectively achieve JIE, the department stated that the National Institute of Standards and Technology and the Office of Personnel Management are to publish a coding structure in response to the Federal Cybersecurity Workforce Assessment Act of 2015. DOD stated that this structure is to inform steps

[39]In December 2014, the *Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015* included provisions commonly referred to as the *Federal Information Technology Acquisition Reform Act*. According to the provisions, the CIO of covered agencies, which do not include DOD, is to approve the information technology budget request of the covered agency. For DOD, the act states that the DOD CIO is to review and provide recommendations to the Secretary of Defense on the information technology budget request of the department.

DOD plans to take to identify the type of personnel and specific skills required to support enterprise operations and services and the governance capabilities needed to effectively achieve JIE.

In addition, for the recommendation to develop a strategy and schedule to transition JRSS to the Risk Management Framework, the department stated that it expects to complete steps to transition JRSS to the framework by March 2017. By developing and approving a strategy and schedule, the department will be mitigating risks of transition delay and a deficient security posture.

However, we are concerned that the steps the department described for addressing the remaining recommendations may not be sufficient. Specifically,

- We recommended that DOD develop a reliable JIE cost estimate and baseline. In response to our recommendation, DOD said that it will provide cost estimates and baselines for JRSS and Mission Partner Environment—Information System by December 2016. The department also stated that it will add cost baselines for other efforts comprising the JIE framework as those solutions are established. If DOD's cost estimates are consistent with the best practices described in our report and the defined scope of JIE, these steps may assist the department in addressing our recommendation. However, because DOD did not describe how it will develop a reliable JRSS cost estimate and baseline, and because JRSS is a key component of the JIE, it is therefore not clear how the department will develop a reliable overall JIE cost estimate. As noted in our report, it is important to develop an overall cost estimate that can be used to monitor and control the program and component project costs.
- We also recommended that the department develop a reliable JRSS cost estimate and baseline, consistent with best practices described in this report. However, in its response DOD did not specifically indicate how it will address the action called for by our recommendation. The department only stated that it provided us with resource estimates for fiscal years 2014 through 2021, and that the estimates make up the approved JRSS resource baseline. The department added that fiscal year 2017 and fiscal year 2018 spend plans are being reviewed by the DOD components and the Cost Assessment and Program Evaluation office and will be presented to the Executive Committee for approval by December 2016. However, the information DOD provided did not constitute a reliable JRSS cost estimate or baseline. Without a reliable

cost estimate and baseline, DOD lacks important information for monitoring and controlling the JRSS effort.

- Regarding our recommendation that DOD develop a JIE schedule management plan and reliable schedule, the department stated that schedules, including for JRSS, have been developed and will be approved by the Executive Committee by December 2016. The department added that it is in the process of determining solutions for other elements of the JIE framework and that schedules for these initiatives will be reviewed by stakeholders and approved when they have been determined. However, while an overall JIE schedule would be informed by the schedules of its individual components, our recommendation addressed developing a schedule for JIE as a whole. Among other things, developing such a schedule helps support activities such as identifying a critical path, which is necessary for examining the effects of any schedule changes associated with individual JIE components.
- We also recommended that DOD develop a JRSS schedule management plan and reliable JRSS schedule and baseline, consistent with practices described in this report. In its comments, the department stated that a JRSS schedule has been firmed up and that a Migration Planning Board is being established to deal with schedule variances and its charter will be presented to the Executive Committee for approval by December 2016. However, DOD's response did not include actions that specifically address our recommendation. Without a schedule management plan and a reliable schedule and schedule baseline, the department lacks, among other things, assurance that the schedule is not being changed to match performance, which hinders its ability to measure actual performance relative to expected baselines.
- Finally, in response to our recommendation that DOD develop a strategy for conducting JIE security assessments and a schedule to complete the assessments, the department stated that the team that was established to review the security architecture meets the requirement. However, the department did not address the need for a strategy or a schedule. Without a strategy that identifies the resources needed to execute the strategy and the responsible organizations, and a schedule to complete the assessments, the department lacks assurance that the required assessments will be completed.

DOD also provided technical comments, which we have incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the DOD CIO, and the Director of the Office of Management and Budget. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact me at (202) 512-4456 or chac@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made contributions to this report are listed in Appendix III.

Carol C. Harris
Director
Information Technology Acquisition Management Issues

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Thad Cochran
Chairman
The Honorable Richard Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Rodney Frelinghuysen
Chairman
The Honorable Pete Visclosky
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine (1) the extent to which the Department of Defense (DOD) has effectively established scope, cost, and implementation plans for the Joint Information Environment (JIE) and (2) the extent to which DOD is executing effective executive oversight and governance of JIE.

To determine the extent to which DOD has effectively established JIE scope, cost, and implementation plans, we reviewed DOD's efforts to establish scope and a reliable cost estimate and baseline, and to perform key implementation planning activities. These planning activities included establishing a reliable schedule and schedule baseline, and developing JIE workforce and security assessment plans. In addition, we reviewed the department's efforts to estimate and establish cost and schedule baselines and develop security plans for the Joint Regional Security Stacks (JRSS), which DOD officials reported as being the current focus of the JIE effort.

To evaluate JIE scope, we reviewed the latest JIE implementation strategy, dated September 2013, and briefings delivered by the Office of the DOD Chief Information Officer (CIO) to congressional staffers and to us, and compared this documentation with leading program planning practices.[1] These practices include developing a detailed program scope statement, which is verified and approved by stakeholders, and developing a plan for managing the scope throughout the program. In addition, we discussed JIE scope with officials from relevant DOD entities, including the Office of the CIO, Defense Information Systems Agency (DISA), and the Departments of the Air Force, Army, and Navy to obtain their perspectives.

To evaluate the JIE cost estimate and cost baseline, we compared DOD's efforts to develop and establish a JIE cost estimate baseline with leading program management practices that call for developing an overall cost baseline and monitoring and controlling program and project costs,[2] as

[1]Project Management Institute, Inc., *The Standard for Program Management –Third Edition* (Newtown Square, Pa.: 2013).

[2]Project Management Institute, Inc., *The Standard for Program Management–Third Edition,* 2013.

well as a requirement in the *National Defense Authorization Act for 2013* that DOD assess the resources needed to achieve JIE.[3]

For the JRSS cost estimate and cost baseline, we compared DOD's most recent JRSS cost estimate, dated September 2015, and supporting documentation with relevant cost baselining and estimating guidance and practices. Specifically, we compared it with leading project management practices[4] and Defense Information Systems Agency guidance[5] that calls for establishing a cost baseline for effective cost management. We also compared the cost estimate with the four characteristics of a reliable estimate described in our *Cost Estimating and Assessment Guide*[6] to determine the extent to which the cost estimates reflected each of these four characteristics: well-documented, comprehensive, accurate, and credible. In addition, we discussed JIE and JRSS cost information with DOD entities, including the Office of the CIO; Defense Information Systems Agency; Office of the Director, Cost Assessment and Program Evaluation, and other officials to obtain their comments on how the cost estimates were developed.

To evaluate the JIE and JRSS schedule and schedule baselines, we compared the JIE and JRSS integrated master schedules with leading schedule management practices identified in our *Schedule Assessment Guide*.[7] We also compared the integrated master schedules with the JIE Implementation Strategy and 2015 JRSS Implementation Plan. In

[3]*National Defense Authorization Act for Fiscal Year 2013*, Pub. L. No. 112-239, § 931, 126 Stat. 1632, 1883 (Jan. 2, 2013).

[4]Project Management Institute, Inc. *The Standard for Program Management—Third Edition (Newtown Square, Pa.: 2013)* and *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)—Fifth Edition*, 2013. See also GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C. March 2009).

[5]Defense Information Systems Agency, *Information Services Acquisition Oversight and Management*, DISA Instruction 610-225-2 (Feb. 19, 2015) and *DISA IT Acquisition Guide: Proactively Tailored Acquisition Models and Processes to Guide DISA's Acquisition of IT Products and Services*, Version 1.0 (Nov. 1, 2013).

[6]GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C., March 2009).

[7]GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: December 2015).

addition, we met with officials from the Office of the DOD CIO and the Defense Information Systems Agency to discuss their process for developing and managing the schedule, and the extent to which this process has been documented.

To evaluate the workforce planning efforts, we reviewed and analyzed key department workforce planning documents, such as the March 2014 JIE Personnel Plan, the draft DOD Cyberspace Workforce Framework, and the November 2015 JRSS Implementation Plan. We also reviewed leading practices for effective workforce planning documented in prior GAO work on human capital planning,[8] workforce planning requirements identified in DOD's Integrated Capabilities Document for JIE, and requirements contained in the *National Defense Authorization Act for Fiscal Year 2013*.[9] We then assessed the extent to which the department's workforce planning activities adhered to these identified best practices, agency documentation, and legislative requirements. For example, we reviewed and analyzed the draft framework to ascertain the extent to which DOD had documented the skills, competencies, and work roles needed for JIE.

To evaluate DOD's security plans for JIE and JRSS, we reviewed JIE Execute Orders and DOD security guidance[10] and assessed JIE and JRSS security plans and schedules relative to these orders and guidance as well as National Institute of Standards and Technology standards and guidance.[11] Further, we interviewed officials from the Office of the CIO, United States Cyber Command, Defense Information Systems Agency, Joint Interoperability Test Command, and the Office of the Director, Operational Test and Evaluation, about JIE and JRSS security plans.

[8]GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[9]Pub. L. No. 112-239, § 931, 126 Stat. 1883.

[10]Department of Defense, *DOD Instruction on Cybersecurity* (8500.01), March 14, 2014, and *DOD Instruction on Risk Management Framework for DOD Information Technology* (8510.01), March 12, 2014.

[11]National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems* Special Publication 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

To determine the extent to which DOD is executing effective executive oversight and governance of JIE, we reviewed the JIE Management Construct Charter to determine the roles and responsibilities assigned to the JIE Executive Committee and its members. We also reviewed meeting minutes and presentations and compared the committee's approach with leading governance and oversight practices documented in our *Information Technology Investment Management Maturity Framework*,[12] the *Capability Maturity Model® Integration for Acquisition* and *Capability Maturity Model® Integration for Development*,[13] and Project Management Institute guidance.[14] We also reviewed information on action item tracking and interviewed the JIE Executive Committee tri-chairs, including officials from Office of the CIO, the Joint Staff CIO, and United States Cyber Command to discuss the governance and overseeing of JIE. In addition, we met with executive committee members, including officials from the Office of the Assistant Secretary for Acquisition, Technology and Logistics, the departments of the Air Force, Army and Navy; and the United States Marine Corps, about their roles and responsibilities for JIE.

We conducted this performance audit from June 2015 to July 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[12]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004). See also GAO, *Immigration Benefits System: Better Informed Decision Making Needed on Transformation Program*, GAO-15-415 (Washington, D.C.: May 2015).

[13]Software Engineering Institute/Carnegie Mellon, *Capability Maturity Model® Integration (CMMI®) for Development*, Version 1.3, CMU/SEI-2010-TR-033 (Hanscomb AFB, Massachusetts: November 2010) and *CMMI® for Acquisition*, Version 1.3, CMU/SEI-2010-TR-032 (Pittsburgh, Pa.: November 2010).

[14]Project Management Institute, Inc., *The Standard for Program Management –Third Edition*, 2013.

Appendix II: Comments from the Department of Defense

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

Ms. Carol Cha
Director, Information Technology
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Cha:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-16-593, 'JOINT INFORMATION ENVIRONMENT: DOD Needs to Strengthen Governance and Management,' dated May 24, 2016 (GAO Code 100126).

Thank you for the opportunity to comment on this draft report. The Department appreciates the work performed by the Government Accountability Office in auditing the Joint Information Environment (JIE). The JIE is critical to enabling DoD to meet its National Defense Mission.

DoD is pleased to note GAO's recognition of the work the Department has done since 2012 to achieve the JIE. The nine recommendations in the draft report provide the Department a different perspective for evaluating JIE and identify several opportunities to improve the management of the various efforts that comprise JIE. DoD is committed to continue working with the GAO to ensure the effective performance of the JIE which is bringing about revolutionary capabilities and efficiencies to DoD.

Should you have any questions, please contact Mr. Roger Thorstenson, roger.k.thorstenson.civ@mail.mil, 571-372-4427.

Sincerely,

DE VRIES.DAVID.LEE.1093968235
Digitally signed by DE VRIES.DAVID.LEE.1093968235
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OSD, cn=DE VRIES.DAVID.LEE.1093968235
Date: 2016.06.20 10:59:56 -04'00'

David L. De Vries
Principal Deputy

Enclosure:
DoD Comments to the GAO Recommendations

GAO DRAFT REPORT DATED MAY 24, 2016
GAO-16-593 (GAO CODE 100126)

"JOINT INFORMATION ENVIRONMENT: DOD NEEDS TO STRENGTHEN GOVERNANCE AND MANAGEMENT"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

Overarching Response: Each of the GAO recommendations begins with the statement, "The GAO recommends that the Secretary of Defense direct the appropriate entities to…," which has resulted in the Department's response of "Partially Concur" for each of the recommendations. The responsible entity for implementing the JIE is the DoD CIO as directed by the Deputy Secretary of Defense's May 6, 2013 memo, "Joint Information Environment Implementation". Where fiscally and technically feasible, the recommendations in the draft report will be applied.

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the appropriate entities to develop a detailed JIE scope statement that is verified by stakeholders and approved by the Executive Committee.

DoD RESPONSE: Partially Concur. A JIE scope statement has been issued to the Department; however, the DoD CIO is in the process of completing an updated JIE scoping document for stakeholder review and JIE Executive Committee (EXCOM) approval by December 2016.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the appropriate entities to establish a plan for managing, documenting, and communicating scope.

DoD RESPONSE: Partially Concur. The DoD CIO is in the process of completing an updated scoping document for JIE by December 2016, which further defines the scope of JIE. This new document will more clearly enable reporting, tracking and controlling of DoD's Information Technology (IT) Modernization activities. The document will specify a process for communicating JIE scope updates.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense direct the appropriate entities to develop a reliable JIE cost estimate and baseline, consistent with the best practices described in this report;

DoD RESPONSE: Partially Concur. The Joint Regional Security Stack (JRSS) and the associated network upgrades, and Mission Partner Environment—Information System (MPE-IS) are clearly defined modernization efforts with firmly established suites of equipment, locations and quantities. DoD will provide cost estimates and baselines for these efforts by December 2016. Other IT Modernization efforts comprising the JIE Framework are still being assessed to determine the appropriate approaches that will improve the Department's operational effectiveness and security and drive down cost. As solutions for these IT modernization efforts are established, cost baselines for these areas will be added, as appropriate.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense direct the appropriate entities to develop a reliable JRSS cost estimate and baseline, consistent with practices described in this report.

DoD RESPONSE: Partially Concur. The JRSS Program Manager provided GAO JRSS cost estimate information. In addition, DoD CIO provided GAO with JRSS resource estimates for FY14 through FY21. Those estimates make up the approved JRSS resource baseline. The FY17 and FY18 spend plans are being reviewed by the DoD Components and Cost Assessment and Program Evaluation (CAPE) and will be presented to the JIE EXCOM for approval by December 2016.

RECOMMENDATION 5: The GAO recommends that the Secretary of Defense direct the appropriate entities to develop a JIE schedule management plan and reliable schedule, consistent with practices described in this report.

DoD RESPONSE: Partially Concur. Some elements of JIE, such as, JRSS and the associated network upgrades and MPE-IS development are well defined, have discrete tangible deliverables, and lend themselves to tight scheduling. Additionally, these initiatives comprise the highest priority objectives of JIE. Schedules for these initiatives have been developed and have been approved by the JIE EXCOM by December 2016.

Other elements of the JIE Framework are involved in analysis and risk reduction efforts that are necessary before determining the appropriate mix of solutions that will provide the required improvements in efficiency, operational effectiveness and security. Solutions and associated schedules for these JIE initiatives will be reviewed by stakeholders and approved by the JIE EXCOM when they have been determined.

RECOMMENDATION 6. The GAO recommends that the Secretary of Defense direct the appropriate entities to develop a JRSS schedule management plan and reliable JRSS schedule and schedule baseline, consistent with practices described in this report.

DoD RESPONSE: Partially Concur. The JRSS schedule has been firmed up and a JRSS Migration Planning Board (MPB) is being established to deal with schedule variances. The MPB charter will be presented to the JIE EXCOM for approval by December 2016.

RECOMMENDATION 7: The GAO recommends that the Secretary of Defense direct the appropriate entities to complete an assessment to determine the number of staff and the specific skills and abilities needed to effectively achieve JIE, consistent with the workforce planning practices described in this report.

DoD RESPONSE: Partially concur. Sections 301-305 of Public Law (PL) 114-113, the "Federal Cybersecurity Workforce Assessment Act of 2015," outline the requirements for a federal-wide cyber workforce coding initiative that will affect both DoD civilian and military cyber personnel. This legislation requires that the National Institute of Standards and Technology (NIST) and Office of Personnel Management (OPM) publish a coding structure aligned to the National Initiative for Cybersecurity Education by June 2016, which will enable

the Federal Government to code IT, cybersecurity, and other cyber-related functions. This initiative requires an examination of all cyber positions and identification of work roles/tasks associated with each job. The Department will use the resulting data to enhance management of the DoD cyber workforce, to include development of qualification requirements for each work role. This, in turn, will inform identification of the type of personnel and specific skills required to support enterprise operations and services and the governance capabilities needed to achieve JIE effectively. Coding of the federal civilian cyber workforce is to be completed by December 2017, and the military cyber workforce by December 2018, in accordance with PL 114-113.

RECOMMENDATION 8: The GAO recommends that the Secretary of Defense direct the appropriate entities to develop a strategy for conducting JIE security assessments that describes the resources needed to execute the strategy, responsible organizations, and a schedule to complete the assessments.

DoD RESPONSE: Partially Concur. At the direction of the DoD CIO, the Department's NIPRNet / SIPRNet Cyber Security Architecture Review (NSCSAR) is being conducted by DoD CIO, the National Security Agency (NSA), and the Defense Information Systems Agency (DISA). In coordination with other DoD Components NSCSAR is the initiative that meets this requirement. It makes recommendations as to where cybersecurity capabilities are best positioned in the architecture to provide the greatest operational effect or makes recommendations to that end. NSCSAR assessments of the DoDIN within the JIE framework, will be delivered incrementally.

RECOMMENDATION 9: The GAO recommends that the Secretary of Defense direct the appropriate entities to develop a strategy and schedule to transition JRSS to the Risk Management Framework, and develop the security plan required by the new framework.

DoD RESPONSE: Partially Concur. The strategy and schedule to transition to the Risk Management Framework (RMF) is in effect. Currently the SIPRNet RMF package is scheduled to be completed by July 2016 and is expected to be approved Sep 2016. The NIPRNet package will inherit many of the SIPRNet controls with target completion by March 2017.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris, (202) 512-4456 or ChaC@gao.gov

Staff Acknowledgments

In addition to the contact above, individuals making contributions to this report include Michael Holland (Assistant Director), Cheryl Dottermusch (Analyst-in-Charge), Camille Chaires, Nancy Glover, James Houtz, Carlo Mozo, Monica Perez-Nelson, Adam Vodraska, and Alyssa Weir.